UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/623,112	07/18/2003	Gary G. Liu	10664-166001	4468

26181 7590 11/09/2007

FISH & RICHARDSON P.C.
PO BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
LI, GUANG W	

ART UNIT	PAPER NUMBER
2146	

MAIL DATE	DELIVERY MODE
11/09/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/623,112	LIU, GARY G.	
	Examiner	Art Unit	
	Guang Li	2146	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 August 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-58* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-58* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *10/09/2007*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. It is hereby acknowledged that the following papers have been received and placed of record in the file: Amendment date 08/20/2007.

2. Claims 1-58 are presented for examination.

Information Disclosure Statement

3. As required by **M.P.E.P. 609(C)**, the applicant's submissions of the Information Disclosure Statements dated 10/09/2007 is acknowledged by the examiner and the cited references have been considered in the examination of the claims now pending. As required by **M.P.E.P 609 C(2)**, a copy of the PTOL-1449 initialed.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1-14, 20-27, 33-44 and 53-58 are rejected under 35 U.S.C. 102(e) as being anticipated by Pickup (US 2003/01212791 A1).

6. Regarding claim 1, Pickup teaches a method for detecting spam in a messaging system (a method of authorising electronic mail that utilises a recipient's list of authorised senders see abstract) comprising:

generating a white list of confirmed message senders (updating a whitelist containing details of a recipient's authorised senders see ¶[0026]), each of said confirmed message senders being authorized to send messages as evidenced by prior receipt of a response to a confirmation message ("the sender is added to the list of authorised senders and the electronic mail is forwarded to the recipient" see¶[0011]);

sharing the white list among a plurality of spam filters (Spam filter as recipient "each recipient has a list of authorized senders" see¶[0016]) in the messaging system (share the same list of authorized senders in each recipient "there are a plurality of recipients, and **each recipient has a list of authorised senders**. In an alternative form to this, **a plurality of recipients share the same list of authorised senders**" see¶0016]);

using the white list at a given one of the plurality of spam filters to determine if a sender of a received message has been previously confirmed ("the request for verification sent to the recipient can be forwarded only if received within a predetermined time of the recipient sending a message to the sender. This will allow the recipient to "match" requests for verification with emails that they have previously sent" see ¶[0021]); and

forwarding the received message to a recipient without separately confirming the sender if it is determined that the sender has been previously confirmed ("Where verification is received, the sender is added to the recipient's whitelist and further emails from the sender can be delivered to the recipient without the requirement for a verification step" see ¶0063]).

7. Regarding claim 2, Pickup teaches the method of claim 1 wherein the messaging system is an email system (system for authorizing electronic mail see ¶[0001]).

8. Regarding claim 3, Pickup teaches the method of claim 1 wherein sharing the white list includes sharing the white list with at least two spam filters (two or more recipients share the same list "there are a plurality of recipients, and each recipient has a list of authorised senders. In an alternative form to this, a plurality of recipients share the same list of authorised senders" see¶0016]).

9. Regarding claim 4, Pickup teaches the method 1 wherein if the sender has not been previously confirmed (a system for authorising electronic mail sent by an unauthorised sender to a recipient see ¶[0035]), the method further includes:

sending a confirmation to the sender (send a request for verification to the sender of an unauthorised email see ¶[0039]);

verifying a response from the sender (wherein upon receipt of the verification from the sender see ¶[0040]); and

if the response is verified, adding the sender to the white list at the given spam filter (the whitelist is modified to include the sender's details and the electronic mail is forwarded to the recipient see ¶[0040]) and sharing the information associated with the added sender with other spam filters in the messaging system (In an alternative form to this, a plurality of recipients share the same list of authorised senders" see¶0016]).

10. Regarding claim 5, Pickup teaches the method of claim 1 wherein sharing includes publishing the white list at a central location (system-wide whitelist sender and global whitelist see ¶[0064]).

11. Regarding claim 6, Pickup teaches the method of claim 1 further comprising maintaining the white list at a central location wherein using the white list includes checking the white list maintained at a central location (the whitelist at the server will be automatic update and share with other recipients "To automatically update the whitelist, the recipient can utilise the automatic updating mechanism of the present invention" see ¶[0062]).

12. Regarding claim 7, Pickup teaches the method of claim 1, wherein the if the sender has not been previously confirmed, the method further comprising:

sending a confirmation to sender(send a request for verification to the sender of an unauthorised email see ¶[0039]);

verifying a response from the sender(wherein upon receipt of the verification from the sender see ¶[0040]); and

if the response is verified, adding the sender to the white list maintained at a central location (the whitelist is modified to include the sender's details and the electronic mail is forwarded to the recipient see ¶[0040]) that is shared among the plurality of spam filters (In an alternative form to this, a plurality of recipients share the same list of authorised senders" see¶0016]).

13. Regarding claim 8, Pickup teaches a method for identifying a spam message (a method of authorising electronic mail that utilises a recipient's list of authorised senders see abstract) comprising:

receiving a message at a spam filter in a network that includes a plurality of spam filters, each spam filter having an associated list of confirmed senders (share the same

list of authorized senders in each recipient "there are a plurality of recipients, and **each recipient has a list of authorised senders**. In an alternative form to this, **a plurality of recipients share the same list of authorised senders**" see¶[0016]);

Identifying the sender of the message (check the message after receiving message see Fig.1) ;

determining if the sender has been previously confirmed as a confirmed sender including (Check to see whether the sender is belong to whitelist sender see Fig.1):

determining if the sender is includes a list of confirmed senders associated with at least one spam filter in the network (Check the System-wide white sender list where all the recipients share authorizes list of users see Fig.1) ;

if it is determined that the sender is not included in the list of confirmed senders associated with the at least one spam filter, determining if the sender is included in a list of confirmed senders associated with another one of a plurality of spam filters; and If it is determined that the sender is included in a list of confirmed senders associated with anyone of the spam filter (If the list not in the system-wide whitelist sender block and process to recipient white list block to see sender is in the recipient whitelist sender see Fig.1) ; and

then forwarding the received message to a recipient without separately confirming the sender in each spam filter (If the sender in the system-wide whitelist sender or recipient whitelist sender, the message will deliver email to recipient see Fig.1).

14. Regarding claim 9, claim 9 is rejected for the same reason in claim 2 as set forth hereinabove.

15. Regarding claim 10, Pickup teaches the method of claim 8 further comprising sharing a list of confirmed senders associated with one spam filter with another spam filter (the list of authorized is share with recipient "In an alternative form to this, a plurality of recipients share the same list of authorised senders" see¶0016]).

16. Regarding claim 11, Pickup teaches the method of claim 8, wherein if is determined that the sender has not been previously confirmed (a system for authorising electronic mail sent by an unauthorised sender to a recipient see ¶[0035]), the method further comprising:

sending a confirmation to the sender(send a request for verification to the sender of an unauthorised email see ¶[0039]);

verifying a response from the sender(wherein upon receipt of the verification from the sender see ¶[0040]); and

if the response is acceptable, adding the sender to the list of confirmed senders an associated spam filter (the whitelist is modified to include the sender's details and the electronic mail is forwarded to the recipient see ¶[0040]) and sharing information with other spam filters in the network, the information including information indicating that the sender has been confirmed (In an alternative form to this, a plurality of recipients share the same list of authorised senders" see¶0016]).

17. Regarding claim 12, Pickup teaches the method of claim 11 wherein sharing information with other spam filters includes publishing the list of confirmed senders at a

central location that can be accessed by the spam filters (system-wide whitelist that can be access from all the recipients see Fig.1 System-wide whitelist sender).

18. Regarding claim 13, Pickup teaches the method of claim 8 further comprising maintaining each list of confirmed senders at a central location (the mail server is located outside of a network associated with the recipient see ¶[0047]), wherein determining if the sender has been previously confirmed includes checking at least one list of confirmed senders at the central location (the whitelist at the server will be automatic update and share with other recipients "To automatically update the whitelist, the recipient can utilise the automatic updating mechanism of the present invention" see ¶[0062]).

19. Regarding claim 14, Pickup teaches the method of claim 8, wherein if the sender has not been previously confirmed, the method further comprising:

sending a confirmation to the sender (send a request for verification to the sender of an unauthorised email see ¶[0039]);

verifying a response (wherein upon receipt of the verification from the sender see ¶[0040]); and

if the response is acceptable, adding the sender to the list shared among the plurality of spam filters (the whitelist is modified to include the sender's details and the electronic mail is forwarded to the recipient see ¶[0040]).

20. Regarding claim 20, Pickup teaches a method for detecting spam in a messaging system comprising:

generating a list of confirmed message senders (updating a whitelist containing details of a recipient's authorised senders see ¶[0026]) and maintaining the list (To automatically update the whitelist, the recipient can utilise the automatic updating mechanism see ¶[0062]) at a data center (the mail server is located outside of a network associated with the recipient see ¶[0047]);

receiving a message at a spam filter in a network that includes a plurality of spam filters(share the same list of authorized senders in each recipient "there are a plurality of recipients, and **each recipient has a list of authorised senders**. In an alternative form to this, **a plurality of recipients share the same list of authorised senders**" see¶0016]);

verifying with the data center that the sender of the message is a confirmed message sender(system-wide whitelist sender and global whitelist see ¶[0064]) , and

if it is determined that the sender is a confirmed message sender, forwarding the received message to a recipient without separately confirming the sender (the whitelist is modified to include the sender's details and the electronic mail is forwarded to the recipient see ¶[0040]).

21. Regarding claim 21, claim 21 is rejected for the same reason in claim 2 as set forth hereinabove.

22. Regarding claim 22, Pickup teaches the method of claim 20 further comprising sharing the list with at least two spam filters in the network (two or more recipients share the same list "there are a plurality of recipients, and each recipient has a list of

authorised senders. In an alternative form to this, a plurality of recipients share the same list of authorised senders" see¶0016]).

23. Regarding claim 23, Pickup teaches the method of claim 20 wherein if it is determined that the sender is not a confirmed message sender **(system for authorizing electronic mail sent by an unauthorized sender to a recipient see ¶[0035]),** the method further comprising:

sending, from the data center, a confirmation to the sender (forwarding a request for verification to the sender see ¶[0025]); verifying a response received at the data center from the sender (verification means operating, upon detection of an unauthorized email, to send a request for verification to the sender of an authorized email see¶[0039])

if the response is acceptable, adding to the list of confirmed message senders a name associated with the sender(wherein upon receipt of the verification from the sender, the whitelist is modified to include the sender's details and the electronic mail is forwarded to the recipient see ¶[0040]); and sharing information including the name with other spam filters in the network (a plurality of recipients share the same list of authorised senders see¶0016]).

24. Regarding claim 24, Pickup teaches a method for identifying a spam message (a method of authorising electronic mail that utilises a recipient's list of authorised senders see abstract) comprising:

Receiving a message at a spam filter in a network that includes a plurality of spam filters (share the same list of authorized senders in each recipient "there are a

plurality of recipients, and **each recipient has a list of authorised senders**. In an alternative form to this, **a plurality of recipients share the same list of authorised senders**" see¶0016]);

Identifying a sender of the message (check the message after receiving message see Fig.1) ;

Verifying, at a data center (the mail server is located outside of a network associated with the recipient see ¶[0047]) coupled to the spam filters, the sender has been previously confirmed as a confirmed sender including determining if the sender is included in a list of confirmed senders for associated with at least one spam filter in the network, said list maintained at the data center (Verifying the sender is in the system-wide whitelist sender, if not check recipient whitelist sender see Fig.1) ; and

If the sender has been previously confirmed, forwarding the received message to a recipient without separately confirming the sender (the whitelist is modified to include the sender's details and the electronic mail is forwarded to the recipient see ¶[0040]).

25. Regarding claim 25, claim 25 is rejected for the same reason in claim 2 as set forth hereinabove.

26. Regarding claim 26, claim 26 is rejected for the same reason in claim 10 as set forth hereinabove.

27. Regarding claim 27, Pickup teaches the method of claim 24 wherein if the sender has not been previously confirmed, the method further comprising:

Sending, from the data center, a confirmation to the sender (forwarding a request for verification to the sender see ¶[0025]);

verifying a response from the sender is acceptable (verification means operating, upon detection of an unauthorized email, to send a request for verification to the sender of an authorized email see¶[0039]); and

adding a name identifying the sender to the list maintained at the data center (automatic process maintains the whitelist whereby only suitably authorised senders are validated and added to the whitelist see ¶[0052]) .

28. Regarding claim 33, Pickup teaches a method for filtering spam in a messaging system (method of authorizing electronic mail sent by a sender to recipient see abstract) comprising:

confirming that a message sender can receive one or more messages (Send verification request back to sender block see fig.1);

sharing information indicating that the message sender can receive one or more messages among a plurality of spam filters in the messaging system (share the same list of authorized senders in each recipient "there are a plurality of recipients, and **each recipient has a list of authorised senders**. In an alternative form to this, **a plurality of recipients share the same list of authorised senders**" see¶0016]);

using said information at a given one of the plurality of spam filters to determine if a message should be sent to an intended recipient without separately determining whether the message sender can receive one or more messages (wherein upon receipt of the verification from the sender, the whitelist is modified to include the sender's details and the electronic mail is forwarded to the recipient see ¶[0040]).

29. Regarding claim 34, claim 34 is rejected for the same reason in claim 2 as set forth hereinabove.

30. Regarding claim 35, Pickup teaches the method of claim 33 further comprising confirming at a first spam filter in the system that a sender of a message can receive messages ("verification means operating, upon detection of an unauthorized email, to send a request for verification to the sender of an authorized email" see¶[0039]).

31. Regarding claim 36, Pickup teaches the method of claim 35 further comprising receiving the message at a second spam filter (Electronic message received at the first system-wide filters (Whitelist and blacklist) and process to recipient filters (whitelist and blacklist see Fig.1).

32. Regarding claim 37, Pickup teaches the method of claim 35 further comprising sharing information developed by the first spam filter with one or more other spam filters in the messaging system (share the same list of authorized senders in each recipient "there are a plurality of recipients, and **each recipient has a list of authorised senders**. In an alternative form to this, **a plurality of recipients share the same list of authorised senders**" see¶0016]).

33. Regarding claim 38, Pickup teaches the method of claim 37 further comprising sharing the information with a data center (the mail server is located outside of a network associated with the recipient see ¶[0047]) and thereafter allowing access by each of the spam filters in the messaging system to the information (share the system-wide whitelist with all other recipients in the network see ¶[0016]).

34. Regarding claim 39, Pickup teaches the method of claim 33 wherein the information is maintained in a list that includes one or more confirmed message senders ("there are a plurality of recipients, and **each recipient has a list of authorised senders"** see ¶[0016]).

35. Regarding claim 40, Pickup teaches the method of claim 39 wherein the list is shared with a plurality of the spam filters in the messaging system (**a plurality of recipients share the same list of authorised senders**" see¶0016]).

36. Regarding claim 41, Pickup teaches the method of claim 39 wherein the list (System-wide whitelist see Fig.1) is maintained by a data center (the mail server is located outside of a network associated with the recipient see ¶[0047]) accessible by the spam filters in the messaging system (share the system-wide whitelist with all other recipients in the network see ¶[0016]).

37. Regarding claim 42, Pickup teaches the method of claim 41 further comprising sharing the list with a plurality of spam filters in the messaging system (**a plurality of recipients share the same list of authorised senders**" see¶0016]).

38. Regarding claim 43, Pickup teaches the method of claim 42 further comprising maintaining a copy of the list at one or more of the of spam filters in the messaging system (list been keep update in the system-wide whitelist "continuously updating a list of authorized senders to filter unwanted electronic mail" see ¶[0027]).

39. Regarding claim 44, Pickup teaches the method of claim 39 further comprising:

associating a passcode with one or more of the confirmed senders in the list, and

verifying a message received from a sender in the list including verifying the passcode specified by the sender (a non-machine readable code for sender verification "utilise a request for verification where that request includes non-machine readable code to make it difficult for automated verification of the message" see ¶[0022]).

40. Regarding claim 53, Pickup teaches a method for processing messages at a spam filter in a messaging system (a method of authorising electronic mail that utilises a recipient's list of authorised senders see abstract), the messaging system including a plurality of spam filters ("there are a plurality of recipients, and **each recipient has a list of authorised senders**. In an alternative form to this**, a plurality of recipients share the same list of authorised senders**" see¶0016]), the method comprising:

receiving a message for processing, the message from a sender for delivery to an intended recipient (Receive email through the inbound e-mail flowchart deliver email to recipient see Fig.1);

determining if the sender is a confirmed sender including querying a data center to determine if the sender is included in a list of confirmed senders based on information received from any of the plurality of spam filters in the messaging system, where confirmed senders are senders having a verified capability to receive messages("the request for verification sent to the recipient can be forwarded only if received within a predetermined time of the recipient sending a message to the sender. This will allow the recipient to "match" requests for verification with emails that they have previously sent" see ¶[0021]); and

if it is determined that the sender is a confirmed sender (Authorizing user in the system-wide white list or recipient whitelist see Fig.1), enabling transmission of the message to the intended recipient ("Where verification is received, the sender is added to the recipient's whitelist and further emails from the sender can be delivered to the recipient without the requirement for a verification step" see ¶0063]).

41. Regarding claim 54, Pickup teaches a method for processing messages at a spam filter in a messaging system (a method of authorising electronic mail that utilises a recipient's list of authorised senders see abstract), the messaging system including a plurality of spam filters ("there are a plurality of recipients, and **each recipient has a list of authorised senders**. In an alternative form to this**, a plurality of recipients share the same list of authorised senders**" see¶0016]), the method comprising:

receiving a message for processing, the message from a sender for delivery to an intended recipient (Receive email through the inbound e-mail flowchart deliver email to recipient see Fig.1);

determining if the sender is a confirmed sender, including querying a data center to determine if the sender is included in a list of confirmed senders based on information received from any of the spam filters in the messaging system, where confirmed senders are senders having a verified capability to receive messages ("the request for verification sent to the recipient can be forwarded only if received within a predetermined time of the recipient sending a message to the sender. This will allow the recipient to "match" requests for verification with emails that they have previously sent" see ¶[0021]);

if it is determined that the sender is a not a confirmed sender, confirming the sender including sending the sender a notification (automatically requesting that the sender provide a verification to confirm their identity and receiving verification from the sender and adding the sender to the list of authorised senders and delivering the electronic mail to the recipient see ¶[0029-0030]); and

upon receipt of a confirmation from the sender in response to the notification, sharing the sender's confirmed status with the plurality of spam filters in the messaging system including publishing the sender's status to the data center (wherein upon receipt of the verification from the sender, the whitelist is modified to include the sender's details and the electronic mail is forwarded to the recipient and plurality of recipients share the same list of authorized senders see ¶[0016]; ¶[0040]).

42. Regarding claim 55, Pickup teaches a method for minimizing spam in a messaging system, (a method of authorising electronic mail that utilises a recipient's list of authorised senders see abstract), the messaging system including a plurality of spam filters ("there are a plurality of recipients, and **each recipient has a list of authorised senders**. In an alternative form to this, **a plurality of recipients share the same list of authorised senders**" see¶0016]), the method comprising:

receiving a request from one of the spam filters in the messaging system to verify if a sender of a message is a confirmed sender, a confirmed sender being a sender having a verified capability to receive messages, evaluating a list of confirmed senders; and providing a notification to the one spam filter indicating whether the sender's status is confirmed (confirmation and verification of confirmed user "identifying an

unauthorised electronic mail, the unauthorised electronic mail being addressed to the recipient and originating from a sender whose details are not included on the whitelist, forwarding a request for verification to the sender, receiving verification from the sender and including the sender's details on the whitelist" see ¶[0028-0030]).

43. Regarding claim 56, Pickup teaches a method for minimizing spam in a messaging system, (a method of authorising electronic mail that utilises a recipient's list of authorised senders see abstract), the messaging system including a plurality of spam filters ("there are a plurality of recipients, and **each recipient has a list of authorised senders**. In an alternative form to this**, a plurality of recipients share the same list of authorised senders**" see¶0016]), the method comprising:

receiving a request from one of the spam filters in the messaging system to verify if a sender of a message is a confirmed sender, a confirmed sender being a sender having a verified capability to receive messages; evaluating a list of confirmed senders (confirmation and verification of confirmed user "identifying an unauthorised electronic mail, the unauthorised electronic mail being addressed to the recipient and originating from a sender whose details are not included on the whitelist, forwarding a request for verification to the sender, receiving verification from the sender and including the sender's details on the whitelist" see ¶[0028-0030]);

if the sender is not included in the list of confirmed senders , confirming the sender including providing a notification to the sender (Send verification request back to the sender see Fig.1) and

upon receipt of a confirmation from the sender in response to the notification, sharing the sender's status with other spam filters in the messaging system including adding the sender to the list (forwarding a request for verification to the sender and receiving verification from the sender and including the sender's details on the whitelist see ¶[0025-0026]); and

notifying the one spam filter indicating whether the sender's status is confirmed (the plurality of recipients share the same list notify each other whether the sender is authorized user or not "there are a plurality of recipients, and **each recipient has a list of authorised senders**. In an alternative form to this, **a plurality of recipients share the same list of authorised senders**" see¶0016]).

44. Regarding claim 57, Pickup teaches the method of claim 56 wherein the step of confirming the sender is performed by a spam filter (Each recipient have individual whitelist and black list "**each recipient has a list of authorised senders**" see ¶[0016]; Fig.1).

45. Regarding claim 58, Pickup teaches the method of claim 56 wherein the step of confirming the sender is performed by the requesting spam filter (sender went though the inbound e-mail flowchart for filtering service and send verification message back to sender for confirmation see Fig.1).

Claim Rejections - 35 USC § 103

46. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

47. **Claims 15-19, 28-32 and 50-52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pickup (US 2003/0212791 A1) in view of Rounthwaite et al. (US 7,219,148).**

48. Regarding claim 15, Pickup teaches a method for detecting a spammer in a network that includes a plurality of spam filters, the method comprising: collecting information relating to a sender from a plurality of the spam filter (identifying and intercepting an unauthorised electronic mail before delivery to the recipient, the unauthorised electronic mail being identified through a comparison of details of the sender with details contained on a list of authorised senders see ¶[0009]).

Pickup does not explicitly disclose determining a trend n the collected information; and identifying a spammer based on the trend.

Rounthwaite teaches determining a trend in the collected information; and identifying a spammer based on the trend (determining spammer based on the limitations "there may be limitations on the number of messages selected per user or per user per time period, or on the probability of selecting a message from any given user. Without such limits, a spammer could create an account" see col.6 lines 62-66). Rounthwaite further provides the advantage of Users which are identified as spam-fighter are asked to vote on whether a selection of their incoming email messages is individually either legitimate mail or junk mail (see Abstract).

It would have been obvious to one of ordinary skill in the art, having the teachings of Pickup and Rounthwaite before them at the time the invention was made to

modify the method and system for detecting spam of Pickup to include determining a trend n the collected information; and identifying a spammer based on the trend as taught by Rounthwaite.

One of ordinary skill in the art would have been motivated to make this modification in order to improve spam-detecting system based on sender actions in view of Rounthwaite.

49. Regarding claim 16, Pickup together with Rounthwaite taught the method for detecting spam according to claim 15, as described above. Rounthwaite further teaches wherein collecting information includes collecting information relating to a number of messages sent by a sender to unrelated email addresses (there may be limitations on the number of messages selected per user" see col.6 lines 62-63).

50. Regarding claim 17, Pickup together with Rounthwaite taught the method for detecting spam according to claim 15, as described above. Rounthwaite further teaches wherein determining trends includes correlating the messages received by an individual spam filter relating to a same sender (to detect as spammer based on the probability of selecting a message from any given user see col.6 lines 62-65).

51. Regarding claim 18, Pickup together with Rounthwaite taught the method for detecting spam according to claim 15, as described above. Rounthwaite further teaches wherein identifying includes determining that a sender is a spammer if a number of messages sent to unrelated email addresses exceeds a predetermined threshold (the disagreement vote all based on individual user action to vote whether the message is

legitimate or spam "the number disagreements exceeds a threshold level, then the suspect users is consider untrustworthy" see col. 19 lines 54-56).

52. Regarding claim 19, Pickup together with Rounthwaite taught the method for detecting spam according to claim 15, as described above. Rounthwaite further teaches wherein the threshold is time dependent (time period can be set in advance or the message can be held until receipt of a determined number of poll results similar to the message e.g.. from the same IP address or with similar content see col.3 line 67 – col.4 lines 1-3).

53. Regarding claims 28-32, they are rejected for the same reason as claims 15-19. Pickup further teaches collecting information using data center (System-wide whitelist or Global whitelist that hosting in the network for identifying the sender permission see ¶[0064]) .

54. Regarding claim 50, Pickup teaches method for filtering spam ,confirming that a message sender can receive one or more messages (Send verification request back to sender block see fig.1); sharing information indicating that the message sender can receive one or more messages among a plurality of spam filters in the messaging system (a plurality of recipients share the same list of authorised senders" see¶0016]). using said information at a given one of the plurality of spam filters to determine if a message should be sent to an intended recipient without separately determining whether the message sender can receive one or more messages. Pickup further teaches correlating sender-recipient data at a spam filter in the messaging system and determining a list of unacceptable senders using the sender-recipient data and the

determined data (Blacklist see Fig.1); and sharing the list of unacceptable senders with other spam filters in the messaging system (sharing the whitelist and blacklist withal the recipient "a plurality of recipients share the same list of authorised senders" see¶[0016]).

Pickup does not explicitly disclose determining data related to how fast a list of recipients grows for a given sender.

Rounthwaite teaches determining data related to how fast a list of recipients grows for a given sender (determining spammer based on the limitations "there may be limitations on the number of messages selected per user or per user per time period, or on the probability of selecting a message from any given user. Without such limits, a spammer could create an account" see col.6 lines 62-66).

It would have been obvious to one of ordinary skill in the art, having the teachings of Pickup and Rounthwaite before them at the time the invention was made to modify the method for filtering system of Pickup to include determining data related to how fast a list of recipients grows for a given sender as taught by Ref B.

One of ordinary skill in the art would have been motivated to make this modification in order to determining whether the senders is spammer or not based on the statistics in view of Rounthwaite.

55. Regarding claim 51, Pickup together with Rounthwaite taught the method for detecting spam according to claim 33, as described above. Pickup further teaches maintaining a list of recipients for each sender of messages processed by a given spam filter (each recipient has a whitelist and blacklists "each recipient has a list of authorised senders" See¶[0016]; Fig.1) .

56. Regarding claim 52, Pickup together with Rounthwaite taught the method for detecting spam according to claim 33, as described above. Pickup further teaches maintaining the list of recipients for each sender at a data center (the whitelist at the server will be automatic update and share with other recipients "To automatically update the whitelist, the recipient can utilise the automatic updating mechanism of the present invention" see ¶[0062]).

57. **Claims 45-49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pickup (US 7,249,175) in view of Brown et al. (US 2004/0034694 A1).**

58. Regarding claim 45, Pickup teaches a method for filtering spam in a messaging system comprising confirming that message sender can receive one or more message , share information with other plurality of spam filters in the message system, using said information to determined if a message should be send to intended recipient without separately confirmation ("the sender is added to the list of authorised senders and the electronic mail is forwarded to the recipient" see¶[0011]). Pickup further teaches wherein the information is maintained in a list that includes one or more confirmed message senders ("there are a plurality of recipients, and **each recipient has a list of authorised senders"** see ¶[0016]).

Pickup does not explicitly disclose prompting a sender in the list to enter a passcode upon an occurrence of an predefined event.

Brown teaches prompting a sender in the list to enter a passcode upon an occurrence of an predefined event (the process passes to block 808 which depicts the

client email application prompting the sender to enter a passcode for the intended recipient see ¶[0053]). Brown further provides the advantage of recipient client email application, a determination is made regarding whether the passcode is included in the email (see abstract).

It would have been obvious to one of ordinary skill in the art, having the teachings of Pickup and Brown before them at the time the invention was made to modify the method for filtering email system of Pickup to include prompting a sender in the list to enter a passcode upon an occurrence of an predefined event as taught by Brown.

One of ordinary skill in the art would have been motivated to make this modification in order to provide security purpose in view of Brown.

59. Regarding claim 46, Pickup together with Brown taught the method for detecting spam according to claim 45, as described above. Brown further teaches detecting that an email address associated with the sender has been compromised, and prompting the sender to enter the passcode thereafter (the process passes to block 808 which depicts the client email application prompting the sender to enter a passcode for the intended recipient see ¶[0053]; Fig.8 blocks 806-808).

60. Regarding claim 47, Pickup together with Brown taught the method for detecting spam as described above. Brown further teaches receiving a pass code from the confirmed message sender; and verifying the pass code is included in the message prior to forwarding the message from the confirmed message the sender to the intended recipient (sender's client email application inserting a passcode directive that includes

the recipient's passcode as the first line in the body of the email message and transmitting the email to the intended recipient see ¶[0054], Fig.8 Blocks 810-812).

61. Regarding claim 48, Pickup together with Brown taught the method for detecting spam according to claim 47, as described above. Brown further teaches automatically adding the passcode associated with the sender at a time for transmission of a message from the sender in the messaging system (when sender compose an email message, the passcode (save in sender address book see Fig.8 block 806) will added to the email and transmit email to intended recipient see Fig.8)

62. Regarding claim 49, Pickup together with Brown taught the method for detecting spam according to claim 48, as described above. Brown further teaches providing a plug-in module for automatically adding the passcode, the plug-in module adapted to add the passcode prior to transmission to the messaging system (Features that added to adding the passcode to the normal email program that consider as plug in module see Fig.8 and Fig.10).

63. **Claims 1-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Donaldson (US 7,249,175) in view of Rounthwaite (US 7,219,148).**

64. Regarding claim 1, Donaldson teaches a method for detecting spam in a messaging system (a system and method for filtering undesirable e-mail with forged nonexistence sender addresses in real-time without sending a message to that sender see abstract) comprising:

generating a white list of confirmed message senders ("Whitelist DB 1094, which contains individual email addresses that are permitted to bypass further filtering" see col. 11 lines 60-62), each of said confirmed message senders being authorized to send messages as evidenced by prior receipt of a response to a confirmation message (Whitelist contains senders information that already permitted by pass the filtering system "For whitelist entries, mail is permitted only from the named user on the remote host to any user on the local host" see col. 21 lines 2-4);

using the white list at a given one of the plurality of spam filters to determine if a sender of a received message has been previously confirmed (if a sender not in the whitelist it will have through filtering process "whitelisting methods are used, so that a filter can reject all sender addresses that are not included in a local whitelist of permissible addresses" see col.7 lines 58-60); and

forwarding the received message to a recipient without separately confirming the sender if it is determined that the sender has been previously confirmed (Authorized user forward the message to the remote host "the proxy checks if this recipient is the first authorized recipient for this message. If so, the proxy connects to the MTA as shown in step 1640, sends the HELO message received earlier from the remote host, and sends the MAIL From transaction received earlier in step 1413" see col. 41 lines 28-34).

Donaldson does not explicitly disclose sharing the white list among a plurality of spam filters in the messaging system.

Rounthwaite teaches sharing the white list among a plurality of spam filters in the messaging system (the new filter 116 can be distributed on an ongoing basis by a distribution component 118 across participating internet server provider, to the email or message server, to individual email clients, to an update server, and/or to central database of individual companies see col.9 lines 7-11). Rounthwaite further provides the advantage of User which are identified as spam-fighters are ask to vote on whether a selection of their incoming messages is individually with legitimate mail or junk mail (See abstract).

It would have been obvious to one of ordinary skill in the art, having the teachings of Donaldson and Rounthwaite before them at the time the invention was made to modify the detecting spam system of Donaldson to include sharing the white list among a plurality of spam filters in the messaging system as taught by Rounthwaite.

One of ordinary skill in the art would have been motivated to make this modification in order to provide servers/users for more efficient email filtering and reduce resources associated with the junk mail in view of Rounthwaite.

65. Regarding claim 2, Donaldson together with Rounthwaite taught email spam filtering system according to claim 1, as described above. Donaldson further teaches wherein the messaging system is an email system (email filtering system that substantially eliminates security risks and loss of company resources associated with junk mail see col.8 lines 18-21).

66. Regarding claim 3, Donaldson together with Rounthwaite taught email spam filtering system according to claim 1, as described above. Rounthwaite further teaches

wherein sharing the white list includes sharing the white list with at least two spam filters (the new filter 116 can be distributed on an ongoing basis by a distribution component 118 across participating internet server provider, to the email or message servers, to individual email clients, to an update server, and/or to central database of individual companies see col.9 lines 7-11).

67. Regarding claim 4, Donaldson together with Rounthwaite taught email spam filtering system according to claim 1, as described above. Donaldson further teaches wherein if the sender has not been previously confirmed, the method further includes:

sending a confirmation to the sender ; verifying a response from the sender (Reply and response between the Active Filter proxy and Mail host 1900 to confirm whether mail is accepted or not see Fig.19); and

if the response is verified, adding the sender to the white list at the given spam filter and sharing the information associated with the added sender with other spam filters in the messaging system (If reply unsuccessful, it will added to black list and in other word, when connection is open connection will address to the whitelist "If the reply is "250", then the remote host will apparently relay for the proxy, so the proxy rejects the message as indicated in step 1468 and exits, thus closing all connections. In the preferred embodiment, the proxy also writes a system log entry for the rejected message and appends the IP address to the blacklist database (FIG. 7, item 1095). If the reply to the RCPT message 1462 is anything other than "250", then this indicates that the remote host is not an open relay, and so the proxy continues with reception of the message at step 1470" see col.30 lines 15-29).

68. Regarding claim 5, Donaldson together with Rounthwaite taught email spam filtering system according to claim 1, as described above. Rounthwaite further teaches wherein sharing includes publishing the white list at a central location (The newly trained spam filter 742 can then be distributed to other servers as well as client email software interfacing with LAN 712 see col.17 lines 3-14; Fig.7 Block 742 and Fig.8 Block 812) .

69. Regarding claim 6, Donaldson together with Rounthwaite taught email spam filtering system according to claim 1, as described above. Rounthwaite further teaches further comprising maintaining the white list at a central location wherein using the white list includes checking the white list maintained at a central location (training filter in the central database will keep updated "Training and distributing a new or updated spam filter is an ongoing activity" see col.10 lines 43-48) .

70. Regarding claim 7, Donaldson together with Rounthwaite taught email spam filtering system according to claim 1, as described above. Rounthwaite further teaches wherein the if the sender has not been previously confirmed, the method further comprising:

sending a confirmation to sender; verifying a response from the sender (Reply and response between the Active Filter proxy and Mail host 1900 to confirm whether mail is accepted or not see Fig.19); and

if the response is verified, adding the sender to the white list maintained at a central location that is shared among the plurality of spam filters ("the new filter 116 can be distributed on an ongoing basis by a distribution component 118 across participating

internet server provider, to the email or message server, to individual email clients, to an update server, and/or to central database of individual companies" see col.9 lines 7-11).

Response to Arguments

71. Applicant's arguments with respect to claims 1-58 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Guang Li whose telephone number is (571) 270-1897. The examiner can normally be reached on Monday-Friday 8:30AM-5:00PM(EST).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jeff Pwu can be reached on (571) 272-6798. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

November 8, 2007
Guang Li
Patent Examiner

JEFFREY PWU
SUPERVISORY PATENT EXAMINER